

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JONATHAN GABRIELLI,
Plaintiff,
v.
HALEON US INC.,
Defendant.

Case No. [25-cv-02555-WHO](#)

**ORDER DENYING IN PART AND
GRANTING IN PART MOTION TO
DISMISS**

Re: Dkt. No. 18, 22

Plaintiff Jonathan Gabrielli brings this Class Action Complaint against defendant Haleon US Inc. (“Haleon”), one of the world’s largest consumer healthcare businesses, alleging that Haleon intentionally helped third parties collect California users’ private communications in direct contravention to those users’ express instructions. Gabrielli’s theory of liability is that Haleon promised its users that they could “Reject All” cookies when they visited its websites, but that representation was false; instead, Haleon “surreptitiously enabled third-party tracking cookies on the devices of California visitors to the Websites, even after those visitors explicitly rejected and opted out of all such cookies,” violating plaintiffs’ privacy rights. Gabrielli asserts seven causes of action on behalf of himself and a class of California residents who visited various Haleon websites and attempted to reject non-essential cookies during the relevant class period: (1) invasion of privacy; (2) intrusion upon seclusion; (3) wiretapping in violation of the California Invasion of Privacy Act (“CIPA”), Cal. Pen. Code § 631; (4) use of a pen register in violation of CIPA, Cal. Pen. Code § 638.51; (5) common law fraud; (6) unjust enrichment; and (7) trespass to chattels. Haleon has moved to dismiss, arguing that Gabrielli fails to demonstrate injury in fact sufficient for Article III standing for any of his counts, and that his claims are all otherwise implausible.

Gabrielli has demonstrated Article III standing for his claims, and all of his claims are plausible except one. Haleon’s motion is DENIED except with respect to the trespass to chattels claim, which is dismissed with leave to amend.¹

BACKGROUND

Gabrielli brings this proposed class action against Haleon based on allegations that Haleon violated his privacy rights through deceptive tracking and personal data collection practices. To resolve this motion, I take all well-pleaded facts in the Complaint to be true. *Knievel v. ESPN*, 393 F.3d 1068, 1072 (9th Cir. 2005).

A. Haleon’s Websites

Haleon is a consumer healthcare business that operates a number of websites, including “tums.com; advil.com; centrum.com; Theraflu.com; caltrate.com; flonase.com; Sensodyne.com; and emergenc.com.” Class Action Complaint (“Compl.”) [Dkt. No. 1] ¶ 1.² When California consumers visit the Websites, they see a “popup cookie consent banner.” *Id.* The banners disclose that the Websites use cookies.³ *Id.* They also display an option to “Reject All” or “Accept Cookies.” *Id.*

Gabrielli visited the Tums Website to “browse information about the Tums products on or around August 2023.” He visited the Emergenc Website to browse information about the Emergenc products on or around January 2024. He visited the Centrum Website to browse information about the Centrum products on or around November 2023. And he visited the Sensodyne Website to browse information about the Sensodyne products on or around June 2024. Compl. ¶ 63. When he visited the Websites, the Websites “immediately presented him with Defendant’s popup cookie consent banner, which provided the option to select the ‘Reject All’

¹ In light of this Order, discovery may proceed. Defendants shall respond to pending discovery within 30 days (September 28, 2025). This resolves the discovery dispute. Dkt. No. 36.

² Hereafter, these are referred to as “the Websites.”

³ “Cookies” are “small text files sent by a website server to a user’s web browser and stored locally on the user’s device.” Compl. ¶ 15; *see also* Declaration of Megan Suehiro (“Suehiro Decl.”) Ex. A (Haleon’s General Privacy Notice, disclosing to website visitors that “[a] cookie is a small text file that is placed on your hard disk by a server.”).

cookies button.” *Id.* ¶ 64. The consent banner also represented “[w]e use cookies on our websites to give you the most relevant experience by remembering your preferences and repeat visits.” *Id.*

Gabrielli read both representations. *Id.* Then, “consistent with his typical practice of rejecting or otherwise declining the placement or use of cookies and tracking technologies, [Gabrielli] selected and clicked the ‘Reject All’ cookies button.” *Id.* ¶ 65. He states that he believed that selecting the “Reject All” cookies button on the popup cookie consent banner “would allow him to opt out of, decline, and/or reject all cookies and other tracking technologies (inclusive of those cookies that cause the disclosure of user data to third-party advertising networks, analytics services, and/or social media companies for the purposes of providing personalized content, advertising, and analytics services).” *Id.* “In reliance on those representations and promises,” Gabrielli says that “only then did [he] continue browsing the websites.” *Id.*

Despite Gabrielli’s “reject[ion]” of all cookies, HALEON “nonetheless continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing performance, targeting, and social media services, from the Third Parties on his device.” *Id.* ¶ 68. Gabrielli alleges that the cookies stored and/or loaded on users’ devices when they interact with the Websites “are transmitted to those third parties, enabling them to surreptitiously track in real time and collect Website users’ personal information, such as their browsing activities and private communications with Defendant, including the following:

“**Browsing History:** Information about the webpages a Website user visits, including the URLs, titles, and keywords associated with the webpages viewed, time spent on each page, and navigation patterns; **Visit History:** Information about the frequency and total number of visits to the Websites; **Website Interactions:** Data on which links, buttons, or ads on the Websites that a user clicks; **User Input Data:** The information the user entered into the Websites’ form fields, including search queries, the user’s name, age, gender, email address, location, and/or payment information; **Demographic Information:** Inferences about age, gender, and location based on browsing habits and interactions with Websites’ content; **Interests and Preferences:** Insights into user interests based on the types of Website content viewed, products searched for, or topics engaged with; **Shopping Behavior:** Information about the Website products viewed or added to shopping carts; **Device Information:** Details about the Website user’s device, such as the type of device (mobile, tablet, desktop), operating system, and browser type; **Referring URL:** Information about the website that referred the user to the Websites; **Session Information:** Details about the user’s current Website browsing session, including the exact date and time of the user’s session, the session duration and actions taken on the Websites during

that session; **User Identifiers**: A unique ID that is used to recognize and track a specific Website user across different websites over time; and **Geolocation Data**: General location information based on the Website user's IP address or GPS data, if accessible."

Compl. ¶ 18.

Gabrielli states that had he known that Haleon's representations that consumers could "Reject All" cookies were untrue, he would not have used the Websites. *Id.* ¶ 69. He still wishes to "desire to browse content featured on the Websites," but refrains from doing so because of Haleon's alleged misrepresentations. *Id.* ¶ 70.

B. Timing of discovery

Gabrielli contends that all applicable statutes of limitations have been tolled through the delayed discovery doctrine because "[d]espite exercising reasonable diligence, [Gabrielli] was unaware of [Haleon's] fraudulent and unlawful conduct" set forth in the pleadings "due to [its] active concealment of material facts." Compl. ¶ 71. He learned of Haleon's alleged privacy violations "from counsel." *Id.* "On or around March 25, 2024, [Gabrielli] notified [Haleon] of his claims and allegations" asserted in the Complaint via a demand letter. On February 7, 2025, the parties entered into a tolling agreement stating that "[a]ny and all statute of limitations periods and statute of repose periods related to Claimant's alleged claims for damages and other relief against Haleon shall be tolled during the time period commencing on February 7, 2025, and continuing until March 10, 2025." *Id.* ¶ 72.

Gabrielli filed the underlying complaint on March 15, 2025. He states that the defendant has not been prejudiced in its ability to gather evidence for his claims since "the claims asserted [in the Complaint] are substantially similar to those raised in [Gabrielli's] March 25, 2024 letter." *Id.* ¶ 73. Haleon has moved to dismiss all claims. Motion to Dismiss ("Motion") [Dkt. No. 18-1].

LEGAL STANDARD

I. RULE 12(B)(1)

A motion to dismiss filed pursuant to Rule 12(b)(1) is a challenge to the court's subject matter jurisdiction. *See* Fed. R. Civ. P. 12(b)(1). "Federal courts are courts of limited jurisdiction," and it is "presumed that a cause lies outside this limited jurisdiction." *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994). The party invoking the jurisdiction of

1 the federal court bears the burden of establishing that the court has the requisite subject matter
2 jurisdiction to grant the relief requested. *Id.*

3 A challenge pursuant to Rule 12(b)(1) may be facial or factual. *White v. Lee*, 227 F.3d
4 1214, 1242 (9th Cir. 2000). In a facial attack, the jurisdictional challenge is confined to the
5 allegations pled in the complaint. *See Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004). The
6 challenger asserts that the allegations in the complaint “are insufficient on their face to invoke
7 federal jurisdiction.” *See Safe Air Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir.
8 2004). To resolve facial attacks, the court assumes that the allegations in the complaint are true
9 and draws all reasonable inferences in favor of the party opposing dismissal. *See Wolfe*, 392 F.3d
10 at 362.

11 “By contrast, in a factual attack, the challenger disputes the truth of the allegations that, by
12 themselves, would otherwise invoke federal jurisdiction.” *Safe Air*, 373 F.3d at 1039. To resolve
13 factual attacks, the court “need not presume the truthfulness of the plaintiff’s allegations.” *Id.*
14 (citation omitted). Instead, the court “may review evidence beyond the complaint without
15 converting the motion to dismiss into a motion for summary judgment.” *Id.* (same). Once the
16 moving party has made a factual challenge by offering affidavits or other evidence to dispute the
17 allegations in the complaint, the party opposing the motion must “present affidavits or any other
18 evidence necessary to satisfy its burden of establishing that the court, in fact, possesses subject
19 matter jurisdiction.” *St. Clair v. City of Chico*, 880 F.2d 199, 201 (9th Cir. 1989); *see also Savage*
20 *v. Glendale Union High Sch. Dist. No. 205*, 343 F.3d 1036, 1039 n.2 (9th Cir. 2003).

21 **II. RULE 12(B)(6)**

22 A motion to dismiss under Federal Rule of Civil Procedure 12(b)(6) “tests the legal
23 sufficiency of a claim. A claim may be dismissed only if it appears beyond doubt that the plaintiff
24 can prove no set of facts in support of his claim which would entitle him to relief.” *Cook v.*
25 *Brewer*, 637 F.3d 1002, 1004 (9th Cir. 2011) (citation and quotation marks omitted). Rule 8
26 provides that a complaint must contain a “short and plain statement of the claim showing that the
27 pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). Thus, a complaint must plead “enough facts to
28 state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570

(2007). Plausibility does not mean probability, but it requires “more than a sheer possibility that a defendant has acted unlawfully.” *Ashcroft v. Iqbal*, 556 U.S. 662, 687 (2009). A complaint must therefore provide a defendant with “fair notice” of the claims against it and the grounds for relief. *Twombly*, 550 U.S. at 555 (quotations and citation omitted).

In considering a motion to dismiss, the court accepts factual allegations in the complaint as true and construes the pleadings in the light most favorable to the nonmoving party. *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).; *Erickson v. Pardus*, 551 U.S. 89, 93-94 (2007). However, “the tenet that a court must accept a complaint's allegations as true is inapplicable to threadbare recitals of a cause of action's elements, supported by mere conclusory statements.” *Iqbal*, 556 U.S. at 678.

If a Rule 12(b)(6) motion is granted, the “court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (citations and quotations omitted). However, a court “may exercise its discretion to deny leave to amend due to ‘undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party ..., [and] futility of amendment.’ ” *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892–93 (9th Cir. 2010) (alterations in original) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)).

DISCUSSION

I. ARTICLE III STANDING

Haleon seeks to dismiss all seven counts on the grounds that plaintiffs lack Article III standing to bring any of their claims because Gabrielli has not shown sufficient injury in fact. Its argument is based on the Supreme Court decision, *TransUnion LLC v. Ramirez*, 594 U.S. 413, 141 S. Ct. 2190, 210 L. Ed. 2d 568 (2021) (“*TransUnion*”), and the caselaw that has followed *TransUnion*. See Motion 7-10. It does not prevail.

Article III confines the federal judicial power to the resolution of “Cases” and “Controversies.” *TransUnion*, 594 U.S. at 423, 141 S. Ct. at 2203. To establish standing, “a

plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief.” *Id.* (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992)). “The party invoking federal jurisdiction bears the burden of establishing these elements.” *Lujan*, 504 U.S. at 561. If “the plaintiff does not claim to have suffered an injury that the defendant caused and the court can remedy, there is no case or controversy for the federal court to resolve.” *Casillas v. Madison Avenue Assocs., Inc.*, 926 F.3d 329, 333 (CA7 2019) (Barrett, J.). “Where, as here, a case is at the pleading stage, the plaintiff must ‘clearly . . . allege facts demonstrating’ each element.” *Spokeo, Inc. v. Robbins*, 578 U.S. 330, 338 (2016) (internal citation omitted).

Haleon argues that Gabrielli has failed to establish injury in fact because he “fails to allege the collection of any particular information during his visits to the Websites, let alone the collection of sensitive, personal information that would be ‘highly offensive to a reasonable person.’” Motion 8. It contends that to the extent Gabrielli’s allegations merely challenge what the cookies on Haleon’s Websites “could” do or are “enabled” to do, this is insufficient to confer standing upon him and his proposed class. *Id.* It contends that the Supreme Court’s holding in *TransUnion*, where the court held that demonstrating Article III standing requires a plaintiff to demonstrate “a concrete injury even in the context of a statutory violation,” 594 U.S. at 436, overrides the Ninth Circuit’s determination in *In re Facebook, Inc. Internet Tracking Litigation* that violations of a right to privacy have “long been actionable at common law,” and that “[a] right to privacy ‘encompass[es] the individual’s control of information concerning his or her person.’” 956 F.3d 589, 598 (9th Cir. 2020) (“*Facebook*”) (first quoting *Patel v. Facebook*, 932 F.3d 1264, 1272 (9th Cir. 2019), and then quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)).

The Ninth Circuit has not disavowed *Facebook* in the wake of *TransUnion*. See, e.g., *Jones v. Ford Motor Co.*, 85 F.4th 570, 574 (9th Cir. 2023) (citing *Facebook* approvingly). And it makes sense why it has not. The Supreme Court held in *TransUnion* that “various intangible harms can . . . be concrete. Chief among them are injuries with a close relationship to harms

1 traditionally recognized as providing a basis for lawsuits in American courts.” *TransUnion*, 594
 2 U.S. at 425. The Court recognized that “intrusion upon seclusion” is included among those
 3 traditionally recognized harms. *Id.* at 2204 (“Various intangible harms can also be concrete. Chief
 4 among them are injuries with a close relationship to harms traditionally recognized as providing a
 5 basis for lawsuits in American courts . . . [i]ncluding [for example] reputational harms, disclosure
 6 of private information, and intrusion upon seclusion.”).

7 The Ninth Circuit in *Facebook* held that “[v]iolations of the right to privacy have long
 8 been actionable at common law,” and that “[a] right to privacy ‘encompass[es] the individual’s
 9 control of information concerning his or her person.’ ” *supra*, *Facebook*, 956 F.3d at 598 (internal
 10 citations omitted). Statutes like CIPA thus “codify a substantive right to privacy, the violation of
 11 which gives rise to a concrete injury sufficient to confer standing.” *Id.*; *accord In re Google Inc.*
 12 *Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3d Cir. 2019) (“History and
 13 tradition reinforce that a concrete injury for Article III standing purposes occurs when Google, or
 14 any other third party, *tracks* a person’s internet browser activity without authorization.” (emphasis
 15 added)); *see also Jones*, 85 F.4th at 574 (“A statute that codifies a common law privacy right
 16 ‘gives rise to a concrete injury sufficient to confer standing.’ [internal citation omitted]. And this
 17 court has consistently found that ‘[v]iolations of the right to privacy have long been actionable at
 18 common law.’ ” (internal citations omitted)).⁴ In short, the Ninth Circuit has found that each of the
 19 statutory claims brought here codify substantive rights to privacy, which can be violated by
 20 behavior akin to what Gabrielli alleges Halebion is doing with its users’ information. *See Facebook*,
 21 956 F.3d at 598 (so holding for violations of the Wiretap Act, CIPA, CDAFA). And the Supreme
 22 Court held that intangible harms, like disclosure of private information and intrusion upon
 23 seclusion, “can . . . be concrete.” *TransUnion*, at 2204.

24
 25
 26 ⁴ The Hon. Jon S. Tigar recently considered similar claims brought by the same plaintiff against a
 27 different company in *Gabrielli v. Motorola*; Judge Tigar, relying on the authority cited above,
 28 rejected a similar argument by the defendant there that Gabrielli there had “failed to plead injury-
 in-fact” because he “fail[ed] to identify what specific information was transmitted [by the cookies]
 or what damages he suffered.” No. 24-cv-09533-JST, 2025 WL 1939957, *6-7 (N.D. Cal. Jul. 14,
 2025).

Gabrielli alleges that HALEON “permits the Third Parties to use cookies and other tracking technologies to collect, track, and compile users’ Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data.” Compl. ¶¶ 18, 87. These allegations contradict HALEON’s position that Gabrielli merely challenges its practice of *enabling* cookies that *could* collect users’ data; the complaint alleges that HALEON ignored Gabrielli’s rejection of cookies and “continued to cause the placement and/or transmission of cookies along with user data, including those involved in providing performance, targeting, and social media services, from the Third Parties on his device. In doing so, [HALEON] permitted the Third Parties to track and collect Plaintiff’s private communications as Plaintiff browsed the websites.” *Id.* ¶ 68.

As other courts in this Circuit have held in similar cases, I conclude that Gabrielli’s allegations that HALEON deprived him control of personal information regarding his digital activity and profile are enough to show a concrete injury to his right to privacy and, subsequently, Article III standing. *See e.g., Gabrielli v. Motorola*, No. 24-cv-09533-JST, 2025 WL 1939957, *6-7 (N.D. Cal. Jul. 14, 2025) (where the Hon. Jon S. Tigar determined that the same plaintiff had pleaded injury-in-fact on similar claims against a different defendant); *Brown v. Google LLC*, 685 F. Supp. 3d 909, 925 (N.D. Cal. 2023) (where the Hon. Yvonne Gonzalez Rogers held that plaintiffs had established standing where plaintiffs alleged that defendants had collected their data without consent, thereby violating “concrete privacy interests” that statutes like the Wiretap Act and CIPA protected).

The authority HALEON offers for a different conclusion is distinguishable, largely because the cases it cites involved allegations of disclosed IP addresses, in which there is no privacy interest. For example, in *Khamooshi v. Politico LLC*, Magistrate Judge Sallie Kim found that the plaintiffs had not demonstrated injury in fact sufficient to confer upon them Article III standing. -- F. Supp. 3d. --, 2025 WL 1408896 (N.D. Cal. May 13, 2025). The plaintiffs there did not allege that they “rejected” cookies before using Politico’s site, they merely alleged that they had not consented to the use of their data (there, IP addresses) but that Politico disclosed their IP addresses

1 anyway. *Id.* at *3. The court observed that since “a person generally ‘has no legitimate
2 expectation of privacy in information he *voluntarily* turns over to third parties[.]’” and “IP
3 addresses are ‘voluntarily turned over in order to direct the third party’s servers,’” the plaintiffs
4 had no reasonable expectation of privacy in their IP addresses. Accordingly, the “intangible
5 harm” alleged in that case was not sufficient to show Article III standing.

6 *Gabrielli v. Insider, Inc.*, is also factually distinct. There, the court determined that
7 Gabrielli had not demonstrated standing where he alleged that Insider’s installation of a “Tracker”
8 that collected his IP address and sent it to a third party was a violation of the CIPA. No. 24-CV-
9 01566 (ER), 2025 WL 522515, at *1 (S.D.N.Y. Feb. 18, 2025). In that case, as in *Khamooshi*,
10 Gabrielli did not allege he had expressly “rejected” all cookies and that defendant had installed
11 cookies anyway. Additionally, the court in *Insider, Inc.* found no standing because a person has
12 no reasonable expectation of privacy in IP addresses alone. In contrast, courts in this Circuit have
13 repeatedly held that plaintiffs like Gabrielli have a reasonable expectation of privacy in data like
14 what Gabrielli says was tracked and collected when they expressly reject or otherwise fail to
15 consent to the tracking, collection, and/or disclosure of that data.⁵

16 On August 26, 2025, after the hearing on its Motion, Haleon submitted a Notice of Recent
17 Decision (Dkt. No. 37), notifying the court of *Popa v Microsoft Corp.*, -- F.4th -- 2025 WL
18 2448824 (9th Cir. Aug. 26, 2025), which addressed Article III standing in another right-to-privacy
19 class action complaint involving internet tracking technology. My decision here is not
20 inconsistent with the opinion in *Popa*. There, the plaintiff challenged user-tracking practices
21 employed by a website that she visited. She did not challenge the storage and/or transmission of
22 cookies; she challenged the use of something called “session-replay technology,” which, put
23 simply, “allows a business to capture and reproduce customers’ interactions with its website.”

24
25 ⁵ Haleon also argues that Gabrielli has not demonstrated standing because the information that
26 could have been collected was not “personal or sensitive” or that its collection would be “highly
27 offensive” to a reasonable person. Motion 8. Courts regularly refuse to decide at the pleading
28 stage whether information like that which Gabrielli identifies meets the bar for “personal or
sensitive” information under CIPA. Moreover, this argument is intertwined with the merits, and
courts cannot resolve “jurisdictional questions [that] are intertwined with the merits of a claim.”
Bowen v. Energizer Holdings, 118 F. 4th 1134 (9th Cir. 2024); *see also* *Oppo*. 5.

1 *Popa*, at *1.⁶

2 In the complaint, Popa focused on “specific pieces of information” that were allegedly
3 collected by a particular session-replay technology (called Clarity) that she encountered when she
4 browsed a pet supply website. *Id.* at *2. That information included “the date a user visited the
5 website, the device the user accessed the website on, the type of browser the user accessed the
6 website on, the operating system of the device used to access the website, the country where the
7 user accessed the website from, a user’s mouse movements, a user’s screen swipes, text inputted
8 by the user on the website, and how far down a webpage a user scrolls.” *Id.* She brought claims
9 under Pennsylvania’s anti-wiretapping law, and common law claims for “Invasion of Privacy –
10 Intrusion on Seclusion” on behalf of visitors to the website upon which Clarity was deployed. *Id.*

11 The court determined that Popa lacked a “concrete” injury sufficient to support Article III
12 standing. It explained that *TransUnion* “requires a court to assess whether an individual plaintiff
13 has suffered a harm that has traditionally been actionable in our nation’s legal system.” *Id.* at *4.
14 The court held that Popa “d[id] not explain how the tracking of her interactions with the [host
15 website] caused her to experience any kind of harm that is remotely similar to the ‘highly
16 offensive’ interferences or disclosures that were actionable at common law” because she had
17 “identifie[d] no embarrassing, invasive, or otherwise private information collected by Clarity.” *Id.*
18 at *5. The court observed, “the monitoring of Popa’s interaction with [the website] seems more
19 similar to a store clerk’s observing shoppers in order to identify aisles that are particularly popular
20 or to spot problems that disrupt potential sales.” *Id.*

21 Popa’s class action complaint involved different facts than Gabrielli’s. To start, Haleon’s
22 websites involve healthcare, and Popa challenged a pet food supply website’s tracking practices.

23
24 ⁶ As the Ninth Circuit explained, session-replay technology “‘embed[s] snippets of JavaScript
25 computer code’ on a website, ‘which then deploys on each website visitor’s internet browser for
26 the purpose [of] intercepting and recording the website visitor’s electronic communications with
27 ... the website, including their mouse movements, clicks, keystrokes ..., URLs of web pages
28 visited, and/or other electronic communications in real-time.’” *Id.* The court explained that “[t]he
session-replay provider then ‘use[s] those [w]ebsite [c]ommunications to recreate website visitors’
entire visit to’ the website.” *Id.* A primary purpose of this technology is for businesses to access
useful consumer data that provides insight into what parts of the business’s website are “effective”
with customers.

1 Whatever information users’ input into Haleon’s website is likely more sensitive than what the
 2 plaintiffs in *Popa* inputted into those websites. The tracking technologies are also distinguishable,
 3 both in users’ interactions with them and their capabilities. *Popa* never purported to have
 4 expressly “reject[ed]” the tracking technology at issue. Indeed, the session-replay technology was
 5 not alleged to track anything beyond her interactions with the website she chose to visit, and the
 6 information gathered was only alleged to be used by the owner of that website. In contrast,
 7 Gabrielli alleges that the cookies Haleon stores on users’ devices allow third parties “to track and
 8 collect data in real time regarding ... user input data,” which includes “[t]he information the user
 9 entered into the Websites’ form fields, including search queries, the user’s name, age, gender,
 10 email address, location, and/or payment information, demographic information,” and also “device
 11 information, session information, and/or geolocation data.” Compl. ¶¶ 5, 68.

12 Haleon’s website explains what its cookies are capable of. Not only do they employ
 13 “performance cookies,” which allow Haleon to “count visits and traffic sources so [it] can measure
 14 and improve the performance of [its] website[s],” (a feature somewhat akin to the session-replay
 15 technology at issue in *Popa*), and “targeting cookies,” and “social media cookies,” the latter of
 16 which are “set by a range of social media services that [Haleon] added to the site to enable [users]
 17 to share our content with [their] friends and networks ... [and] are capable of tracking [users’]
 18 browser[s] across other sites and building up a profile of [users’] interests.” Compl. ¶ 23 (Haleon
 19 General Privacy Notice).⁷ Haleon warns that the social media cookies “may impact the content
 20 and messages [users] see on other websites[.]” *Id.* Then, Gabrielli says, third parties “analyze and
 21 aggregate this user data ... for their own purposes and financial gain,” and “share user data and/or
 22 user profiles to unknown parties to further their financial gain.” Compl. ¶ 4.

23 Gabrielli’s allegations are sufficient to show Article III standing.

26 ⁷ Haleon General Privacy Notice United States (updated December 22, 2022) (current version
 27 available at <https://www.privacy.haleon.com/en-us/general/general-full-text/>) (the “Privacy
 28 Notice”). According to Gabrielli, Haleon has subsequently updated its Privacy Notice but, “based
 on information and belief,” this version was in effect at the time of Gabrielli’s rejection of cookies
 on the Tums Website. *See* Compl. ¶ 22, n.1.

II. MOTION TO DISMISS

A. Privacy Claims

Claims for intrusion upon seclusion and invasion of privacy under the California Constitution have “similar elements,” and courts therefore “consider the claims together and ask whether: (1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly offensive.” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (“Facebook”) (citing *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272, 287 (2009)). When evaluating whether a reasonable expectation of privacy exists, “courts consider a variety of factors, including the customs, practices, and circumstances surrounding a defendant’s particular activities.” *Id.* (citing *Hill v. NCAA*, 7 Cal. 4th 1, 36 (1994)). The question is “whether a defendant gained ‘unwanted access to data by electronic or other covert means, in violation of the law or social norms.’ ” *Id.* (quoting *Hernandez*, 47 Cal. 4th at 286).

Haleon argues that Gabrielli’s invasion of privacy and intrusion upon seclusion claims must be dismissed because (1) the alleged invasions of privacy do not meet the high bar for an egregious breach of social norms, and (2) the complaint only alleges that cookies installed on users’ devices *could* track information, and not that defendant *did* track that information. *See* Motion 11-13. Neither argument is persuasive.

First, as Judge Tigar recently reaffirmed in *Gabrielli v. Motorola*, and as I noted briefly *supra*, n.4, it is “premature to dismiss Gabrielli’s claims based on a determination of how offensive or serious the privacy intrusion is.” *Motorola*, at *10. “Under California law, courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is.” *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 797 (N.D. Cal. 2019). In determining whether an invasion is “highly offensive,” courts consider “the degree and setting of the intrusion,” along with “the intruder’s motives and objectives.” *Hernandez v. Hillside, Inc.*, 47 Cal. 4th 272, 287 (Cal. 2009). Due to the factually intensive nature of the inquiry, “[c]ourts are generally hesitant to decide claims of this nature at the pleading stage.” *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d at 799. Only if the allegations “show no reasonable expectation of privacy or an insubstantial impact on privacy

1 interests” can the “question of [a serious or highly offensive] invasion [] be adjudicated as a
2 matter of law.” *Hill*, 7 Cal. 4th at 40. In the Complaint, Gabrielli pleads facts of such a nature that
3 I cannot, at this early stage, conclude as a matter of law that the alleged transmission via stored
4 cookies of Gabrielli’s browsing data, visit history, website interactions, geolocation information,
5 user input data (including search terms), and other types of data is not a highly offensive invasion
6 of his reasonable privacy expectation.

7 Moreover, contrary to Haleon’s contention that Gabrielli has only alleged what its cookies
8 could track, not what they did track, the Complaint alleges that even after Gabrielli rejected all
9 cookies, Haleon “continued to cause the placement and/or transmission of cookies along with user
10 data, including those involved in providing performance, targeting, and social media services,
11 from the Third Parties on his device. In doing so, [Haleon] permitted the Third Parties to track and
12 collect Plaintiff’s private communications as Plaintiff browsed the websites.” *Id.* ¶ 68. The motion
13 to dismiss Gabrielli’s invasion of privacy claims is DENIED.

14 **B. CIPA Claims**

15 **1. Statute of limitations**

16 Haleon argues that Gabrielli’s August 2023, November 2023, and January 2024 CIPA
17 claims are time-barred because they were brought more than one year after the alleged violations.
18 It argues that the delayed-discovery doctrine, (which I refer to as the “discovery rule”), does not
19 apply to salvage the claims because Gabrielli was on “actual notice” of Haleon’s Privacy Notice
20 and default use of cookies so that he could have brought his claims earlier. *See* Motion 14-15.

21 CIPA has a one-year statute of limitations that begins to run on the date of collection.
22 *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 136 (N.D. Cal. 2020). Gabrielli alleges that he visited
23 the Tums website in August 2023, the Centrum website in November 2023, and the Emergen-C
24 website in January 2024, making his latest possible filing date for CIPA claims January 2025.
25 Compl. ¶ 63. He filed this complaint in March 2025. Haleon says that this is clearly outside the
26 statute of limitations. Gabrielli responds that his CIPA claims should be equitably tolled given his
27 earlier pursuit of legal remedies, and that the doctrines of delayed discovery and fraudulent
28 concealment apply. Because the discovery rule applies, I do not reach the issues of equitable

1 tolling or fraudulent concealment.

2 The discovery rule “postpones accrual of a cause of action until the plaintiff discovers, or
3 has reason to discover, the cause of action.” *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal. 4th 797,
4 807 (2005). A “plaintiff has reason to discover a cause of action when he or she ‘has reason at
5 least to suspect a factual basis for its elements.’ [] In so using the term ‘elements,’ we do not take
6 a hypertechnical approach to the application of the discovery rule. Rather than examining whether
7 the plaintiffs suspect facts supporting each specific legal element of a particular cause of action,
8 we look to whether the plaintiffs have reason to at least suspect that a type of wrongdoing has
9 injured them.” *Id.* (internal citations omitted). To adequately plead a basis for the discovery rule, a
10 plaintiff must “plead facts to show (1) the time and manner of discovery and (2) the inability to
11 have made earlier discovery despite reasonable diligence.” *Id.* at 808 (internal quotation omitted).

12 Gabrielli argues that considering first, the nature of this case (that is, it is one that is “based
13 on defendants’ use of highly technical proprietary software,” Compl. ¶ 70), second, that he “does
14 not have the technical knowledge necessary to test whether the Websites honored users’ requests
15 to reject all cookies,” and finally that he only “learned of Defendant’s privacy violations from
16 counsel” in February 2024, *see* Compl. ¶ 71, the statute of limitations is tolled based on the
17 discovery rule. He cites my opinion in *Doe v. FullStory, Inc.*, 712 F. Supp. 3d 1244 (N.D. Cal.
18 2024), which is on point. Both cases are based on defendants’ use of highly technical software,
19 and in each case the plaintiff did not learn of the injury until shortly before filing the suit. *See*
20 *FullStory*, 712 F. Supp. 3d at 1255 (holding that the delayed discovery doctrine applied because
21 “[w]hile defendants argue that plaintiff cannot invoke the discovery rule unless she alleges the
22 specific ‘time and manner’ of her discovery, that argument is not persuasive given the type of case
23 this is – based on defendants’ use of highly technical proprietary software – and given plaintiff’s
24 clear statement that ‘the earliest’ plaintiff could have known of her injury was shortly before
25 filing.”). It is sufficient for now, given the circumstances, that Gabrielli says that the earliest he
26 could have known about the purported injury was shortly before filing this lawsuit.

27 Haleon protests that the discovery rule does not save Gabrielli’s claims because it applies
28 only where a plaintiff demonstrates that “a reasonable investigation at [the] time would not have

revealed a factual basis for that particular cause of action.” Motion 14 (citing *Fox v. Ethicon EndoSurgery, Inc.*, 110 P.3d 914, 917 (Cal. 2005)). It argues that since Gabrielli admits that he reviewed (1) the cookie banner, which discloses that “[c]ookies are enabled by default” on the Websites, and (2) Haleon’s Privacy Notice, which further “explained the third-party cookies” used on the Websites, *see* Compl. ¶¶ 1, 22, 69, 142, Gabrielli had “actual notice” of the use of cookies before his website visits. Motion 14. This argument is not persuasive because Gabrielli alleges that he (and putative class members) expressly opted into “rejecting” all cookies when they visited Haleon’s various websites, an option Haleon offered. Compl. ¶ 70. Regardless of whether plaintiffs were aware of a “default” cookie enabling feature, they selected an option that seemingly allowed them to “reject” that default. This contradicts any argument that they had notice of Haleon’s alleged wrongdoing as soon as they visited the websites.

2. Cal. Penal Code § 631(a)

Section 631(a) creates four avenues for relief:

- (1) where a person “by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection ... with any telegraph or telephone wire, line, cable, or instrument”;
- (2) where a person “willfully and without consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit”;
- (3) where a person “uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained”; and
- (4) where a person “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above.”

Javier v. Assurance IQ, LLC, 649 F. Supp. 3d 891, 897 (N.D. Cal. 2023) (quoting Cal. Penal Code § 631).

Gabrielli asserts that Haleon assisted third parties in “wiretapping” his device and/or intercepting his communications with Haleon in violation of CIPA. Compl. ¶¶ 104-123. Haleon takes issue with Gabrielli’s Section 631(a) claim on two grounds. First, it argues that Gabrielli fails to plead intent with respect to aiding and abetting liability under CIPA. It contends that “Plaintiff did not plead facts to suggest that Haleon *intended* to aid and abet a third party’s violation of CIPA.” Motion 17 (emphasis in original). I disagree. The complaint sufficiently

alleges that Haleon intentionally operated its website and assisted third parties in gathering Gabrielli's information. *See* Compl. ¶¶ 1-3, 12; *see also Zarif v. Hwareh.com, Inc.*, No. 23-CV-0565-BAS-DEB, 2025 WL 486317, at *8 (S.D. Cal. Feb. 13, 2025) (explaining that the Ninth Circuit has interpreted the intent standard under the federal Wiretap Act as requiring only that an act be done on purpose, as opposed to being done with knowledge that it is unlawful, and applying that analysis to reject a challenge to Section 631).

Second, Haleon argues that Gabrielli has not alleged the "contents" of any "communication" he made to the Haleon Websites. The "contents" of "any communication" is defined as "any information concerning the substance, purport, or meaning of a communication." 18 U.S.C. §§ 2511(3)(a), 2702(a), 2510(8); *see also Zynga Privacy Litig.*, 750 F.3d 1098, 1107-08. The Ninth Circuit observed in *Zynga* that under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication. *Id.* However, information that is limited to, say, webpage addresses or personally identifying information that identifies a webpage user, does not constitute "contents" because neither qualify as the "substance, purport, or meaning of" a communication. Congress has excluded this sort of "record information" from the definition of "contents." *Zynga*, at 1107; *see also* 18 U.S.C. §§ 2702(c)(6), 2703(c)(2)(A), (B), (E).

As Gabrielli points out in response, search terms and descriptive URLs, like those alleged in the complaint, constitute "contents." *Oppo*. 15-16; *see Heerde v. Learfield Commc'ns, LLC*, 741 F. Supp. 3d 849, 859 (C.D. Cal. 2024) ("[s]earch terms constitute 'contents' of a communication."); *see also Zynga*, 750 F.3d at 1108-09 (explaining URL data may contain communication "contents" if a user's search terms are included). Gabrielli does not merely identify his "interactions" with the Websites as being transmitted to third parties in violation of CIPA, as was the case in *Mikulsky v. Bloomingdale's, LLC*, which Haleon cites in support, *see* Motion 16. 713 F. Supp. 3d 833, 845 (S.D. Cal. 2024) (dismissing CIPA claim where "button clicks, mouse movements, scrolling . . . page navigation, changes to visual elements in the browsers, network requests and more" consist of "record" information). He identifies the

information collected as “the Website user’s affirmative decisions, actions, choices [and] preferences,” including “user input data” such as “search queries, the user’s name, age, gender, email address, location, and/or payment information.” Compl. ¶¶ 18, 117, 118.⁸ That is more than sufficient.

3. Cal. Penal Code § 638.51(a) – “pen registers”

Haleon also argues that Gabrielli has failed to state a claim under Section 638.51 of CIPA because the section applies only to communications through telegraph or telephone. Motion 17 (citing *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 191 (2021)). Section 638.51(a) prohibits any person from “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order.” CIPA defines a pen register as a “device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.” Cal. Penal Code. § 638.50(b) (emphasis added).

Gabrielli’s theory is that the third-party trackers operate as pen registers under Section 638.50 because the trackers are a process and/or device that collect users’ internet protocol (“IP”) addresses. Compl. ¶ 128. Haleon argues that internet technologies are not “pen registers.” Motion 17. This argument has been considered and rejected multiple times. In *Greenley v. Kochava, Inc.*, the court considered the argument that CIPA’s pen register definition applied to only telephone technology, and observed that “the Court cannot ignore the expansive language in the California Legislature’s chosen definition [of pen register],” which is “specific as to the type of data [collected],” but “vague and inclusive as to the form of the collection tool” (i.e. “device or process”). 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023); *see* Cal. Penal Code § 638.50. The court went on to explain that the Legislature’s chosen definition “indicate[d]” that “courts should focus less on the form of the data collector and more on the result.” *Id.* Accordingly, the *Greenley* court

⁸ Haleon argues in a footnote that it “cannot be directly liable under CIPA because ‘[p]arties to a conversation cannot eavesdrop on their own conversation’ and the first clause of section 631(a) does not apply to internet communications.” Motion 15, n.5. I will reject this argument as Judge Tigar did, *see Motorola*, at *11. Gabrielli alleges that the cookies are collecting data on his private activity and information outside of Haleon’s Websites, not his communications involving Haleon.

1 applied the plain meaning of a “process” to the statute to determine that the software development
2 kit at issue constituted a pen register under CIPA: the court observed, “[a] process can take many
3 forms.” *Id.* Other courts have followed suit. *See e.g., Shah v. Fandom, Inc.*, No. 24-CV-01062-
4 RFL, 2024 WL 4539577, at *2 (N.D. Cal. Oct. 21, 2024); *Mirmalek v. Los Angeles Times*
5 *Commc’ns LLC*, No. 24-CV-01797-CRB, 2024 WL 5102709, at *3 (N.D. Cal. Dec. 12, 2024). I
6 reach the same conclusion.

7 Haleon also asserts, in passing, that Gabrielli’s Section 638.1(a) pen register claim cannot
8 coexist with his Section 631(a) wiretapping claim because pen registers “do not record contents,”
9 but wiretaps do. Motion 18, n.7. It says Gabrielli “cannot have it both ways”; from its
10 perspective, he can either claim that cookies captured the “contents” of his communications,
11 giving rise to his Section 631(a) claim, or he can claim that the cookies are unauthorized pen
12 registers, which “by definition do not capture ‘contents’”, to support his Section 638.1(a) claim.
13 *Id.* This argument would lead to the conclusion that any pen register that also recorded the
14 “contents” of users’ information would no longer fall under the protection of Section 638.1(a) of
15 CIPA. That cannot have been the Legislature’s intent.

16 The Hon. Casey Pitts recently considered and rejected a similar argument, noting the
17 statutory ambiguity concerning whether devices that would otherwise constitute pen registers still
18 fall under the section 638.1(a) pen register CIPA provision if they capture “contents” of web
19 users’ communications as well as simply recording or decoding those communications. *See In re*
20 *Meta Pixel Tax Filing Cases*, No. 22-cv-07557-PCP (N.D. Cal. Aug. 6, 2025). He wrote:

21 Here, there is no doubt that the California Legislature, in enacting CIPA, intended “to
22 protect the right of privacy of the people of this state from what it perceived as a serious
23 threat to the free exercise of personal liberties that cannot be tolerated in a free and
24 civilized society. This philosophy appears to lie at the heart of virtually all the decisions
25 construing [CIPA].” *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002) (cleaned up).
26 Recognizing this intent, the California Supreme Court “has instructed courts to interpret
27 CIPA in the manner that ‘fulfills the legislative purpose of CIPA by giving greater
28 protection to privacy interests.’” *Matera v. Google, Inc.*, 15-cv-04062-LHK, 2016 WL
8200619, at *19 (N.D. Cal. 2016) (quoting *Flanagan*, 27 Cal. 4th at 775).

I agree with Judge Pitts that given CIPA’s purpose to protect Californians’ privacy, it seems very
unlikely that the state Legislature meant to permit the installation and implementation of pen
registers “so long as those devices also record the contents of third party’s communications.”

C. Common law claims: fraud, trespass to chattels, and unjust enrichment**1. Fraud**

To plead fraud, a plaintiff must set forth facts showing (1) a misrepresentation or omission of material fact; (2) knowledge of falsity; (3) intent to defraud or to induce reliance; (4) justifiable reliance; and (5) resulting damage. *Heeger v. Facebook, Inc.* 509 F. Supp 3d 1182, 1194 (N.D. Cal. 2020). When brought in a federal action, the Federal Rules of Civil Procedure govern pleading requirements. *See, e.g., Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). “Rule 9(b) requires that, when fraud is alleged, “a party must state with particularity the circumstances constituting fraud....” and “[a]ny averments which do not meet that standard should be ‘disregarded,’ or ‘stripped’ from the claim for failure to satisfy Rule 9(b).” *Id.*, at 1124. “Averments of fraud must be accompanied by ‘the who, what, when, where, and how’ of the misconduct charged.” *Id.*; *see also, Lazar v. Superior Ct.*, 12 Cal.4th 631, 644-45 (1006) (same requirements under California law). General and conclusory allegations are insufficient. *See, e.g., Doutherd v. United Parcel Serv., Inc.*, No. 21-15966, 2022 WL 17582527, at *1 (9th Cir. Dec. 12, 2022).

Haleon argues that Gabrielli’s fraud claim fails for three reasons. First, it contends that he has failed to allege that “the Reject All cookies button was actually false.” Motion 19. It contends that since Gabrielli alleges that “cookies are enabled by default,” I cannot infer from the pleadings that “there were any cookies in process at the time Plaintiff clicked ‘Reject All.’” *Id.* I agree with Gabrielli that this is an argument better suited to summary judgment; for now, his allegations support that Haleon misrepresented its practices with respect to cookies. Haleon allegedly represented to him (and the class) that they could “Reject All” cookies, but that was false; Gabrielli says that Haleon “controls the software code of its websites,” including its cookie banner, and has “control over whether [cookies] are placed on its user’s devices” in the first place,” Compl. ¶¶ 2, 21, 138. Discovery will reveal the truth of these allegations, but they are sufficient to sustain Gabrielli’s claims at the pleading stage.

Second, Haleon argues that Gabrielli has failed to show intent. But because intent may be

alleged generally, *see* Fed. R. Civ. P. 9(b), his allegations are sufficient for now.⁹

Finally, Halem argues that Gabrielli and the putative class have not suffered any actual damage from the purported fraud. Motion 20. Gabrielli says that damages are based on diminution in value of his private and personally identifiable information, and the unauthorized interception of private communications. Compl. ¶ 140. The Ninth Circuit has accepted similar pleadings in data privacy cases to satisfy Article III injury-in-fact for a fraud claim. *See Facebook*, 956 F.3d at 599-600.¹⁰ Gabrielli asserts that the data Halem transmitted via stored cookies, allegedly without the permission of its Website users, had financial value. Halem offers no case to support its argument that Gabrielli's allegations are insufficient to show damages for fraud, at least at the pleading stage. *See* Motion 20-21. The motion to dismiss the fraud claim is DENIED.

2. Trespass to Chattels

In California, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury." *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 455 (N.D. Cal. 2018) (quoting *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559 (1996)). The California Supreme Court has held that the principles underlying the tort apply to allegations of digital trespass. *See Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003). Thus, "[i]n order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage." *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069–70 (N.D. Cal. 2000). A plaintiff may satisfy the damages element by pleading that the trespass "impaired the condition, quality, or value of the personal property."

⁹ Halem does not challenge Gabrielli's satisfaction of the fourth factor, reliance. Gabrielli alleges that he would not have used the Websites were it not for representations that he could "Reject All" cookies. Compl. ¶¶ 69, 70. This is plausible.

¹⁰ In *Facebook*, the Ninth Circuit held that the plaintiffs' allegations that their browsing histories and other tracked and stored data "carr[ie]d financial value" was sufficient to confer upon them Article III standing to bring their common law claims for, *inter alia*, fraud and trespass to chattels. *Id.*

1 *Fields v. Wise Media, LLC*, No. 12-CV05160 WHA, 2013 WL 5340490, at *4 (N.D. Cal. Sept. 24,
2 2013) (citing *Hamidi*, 30 Cal. 4th at 1356).

3 Gabrielli alleges that Haleon's trespass of "Plaintiff's and other users' computing devices
4 resulted in harm to Plaintiff and other users and caused Plaintiff and other users the following
5 damages: a. Nominal damages for trespass; b. Reduction of storage, disk space, and performance
6 of Plaintiff's and other users' computing devices; and c. Loss of value of Plaintiff's and other
7 users' computing devices." Compl. ¶ 161. Haleon reasserts its argument concerning insufficient
8 damages with respect to Gabrielli's trespass claim. Motion 13-14. It insists that his allegations
9 are conclusory, and even if they were credible, they do not identify the kind of harm plaintiffs
10 must show to sustain trespass to chattels claims.

11 While I discredited Haleon's argument with respect to the fraud claim, it is more
12 persuasive when applied to the claim for trespass. As Judge Tigar observed in *Motorola*, " 'it is
13 not obvious how the presence on one's computer of the cookies from the providers' websites
14 would result in any cognizable reduction in storage, disk space, or performance.' " *Motorola*, at *
15 15 (quoting *Doe I v. Google LLC*, 741 F. Supp. 3d 828, 846 (N.D. Cal. 2024)). Other courts have
16 also been unmoved by plaintiffs' attempts to craft trespass claims where the damages alleged
17 reflect those Gabrielli identifies here. *See e.g., Henson v. Turn, Inc.*, 2018 WL 6605624, at *4
18 (N.D. Cal. Dec. 17, 2018) ("[i]t is a matter of common understanding that cookies are miniscule in
19 size and thus incapable of noticeably affecting the performance of modern computers"); *Doe v.*
20 *Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1088 (N.D. Cal. 2023) (dismissing trespass to chattels
21 claims where there was no allegation that functionality in their computing devices was impaired).

22 Gabrielli points out that the Ninth Circuit in *Facebook* held that the plaintiffs there, who
23 brought claims for trespass to chattels, among other common law claims, had alleged sufficient
24 injury-in-fact to confer upon them Article III standing. As discussed above, the plaintiffs' theory
25 of injury in *Facebook* was that their browsing history carried financial value, and its non-
26 consensual retention constituted injury. 956 F.3d at 600-601; *Oppo*. 23-24. This is immaterial for
27 the purposes of determining whether Gabrielli has alleged sufficient damages to sustain a trespass
28 to chattels claim. The court in *Facebook* was addressing Article III standing generally. In

relevant part, it reversed the district court’s decision to dismiss all of plaintiffs’ claims (including their trespass claims) for want of standing; it did not reach the question of damages particular to plaintiffs’ trespass to chattels claim. The closest it came to the issue was observing in a footnote that the plaintiffs’ common law claims for fraud and trespass to chattels did have a damages requirement. *See id.*, 599, n.4. Unless Gabrielli can plausibly allege that the non-consensual storage of cookies by Haleon “impaired the condition, quality, or value of [his computer],” *Hamidi*, 30 Cal. 4th at 1356, this claim does not appear plausible. The motion to dismiss is GRANTED, with leave to amend.

3. Unjust Enrichment

Gabrielli also asserts a claim for unjust enrichment based on Haleon’s “scheme to increase its own profits through a pervasive pattern of false statements and fraudulent omissions.” Compl. ¶ 148. He alleges that “[Haleon] was unjustly enriched as a result of its wrongful conduct, including through its misrepresentation that users could ‘Reject All’ cookies and by permitting the Third Parties to store and transmit cookies on Plaintiff’s and Class members’ devices and browsers, which permitted the Third Parties to track and collect users’ Private Communications, including their browsing history, visit history, website interactions, user input data, demographic information, interests and preferences, shopping behaviors, device information, referring URLs, session information, user identifiers, and/or geolocation data, even after Class members rejected such cookies.” *Id.* ¶ 149. Gabrielli alleges that his and putative class members’ “Private Communications have conferred an economic benefit on [Haleon].” Compl. ¶ 150.

California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss. *See Cty. of San Bernardino v. Walsh*, 158 Cal. App. 4th 533, 542 (2007) (noting that where “a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss, or in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust ... [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched” (quoting Rest., Restitution, § 1, com. e)). Haleon protests that Gabrielli’s unjust enrichment claim fails because he does not allege that he “suffer[ed] any cognizable loss,” nor does he “plausibly

1 establish that Haleon profited from his data.” Motion 21-22. It argues that all Gabrielli alleges is
2 that Haleon “*can* use the data,” not that it *does*, or that it has profited from such use. *Id.*

3 Courts in this District have regularly held that even if plaintiffs have suffered no economic
4 loss from the disclosure of their plausibly private information, they are allowed to proceed through
5 the pleadings stage with a claim for unjust enrichment to recover the gains that a defendant
6 realized from its allegedly improper conduct. *See Hadley v. Kellogg Sales Co.*, 324 F. Supp. 3d
7 1084, 1113 (N.D. Cal. 2018) (Koh, J.); *In re Facebook, Inc., Consumer Priv. User Profile Litig.*,
8 402 F. Supp. 3d 767, 803 (N.D. Cal. 2019) (Chhabria, J.). The motion to dismiss this claim is
9 DENIED.

10 **D. Punitive damages**

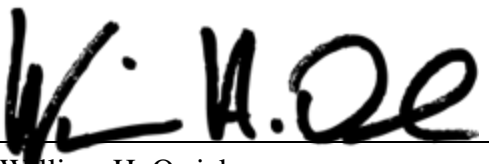
11 Haleon also asks that I dismiss Gabrielli’s request for punitive damages because it fails as
12 a matter of law. Motion 23. To seek punitive damages, Gabrielli must plead facts showing that
13 Haleon acted with “oppression, fraud, or malice” or “evil motive” against him. Cal. Civ. Code §
14 3294(a). As I explained above, Gabrielli’s fraud claim is plausible. *See* discussion *supra* Section
15 II(C)(1). As such, his quest for punitive damages may proceed, for now.

16
17 **CONCLUSION**

18 For the foregoing reasons, the motion to dismiss is DENIED as to all claims except the
19 trespass to chattels claim. The motion to dismiss the trespass to chattels claim is GRANTED, with
20 leave to amend.

21 **IT IS SO ORDERED.**

22 Dated: August 29, 2025

23
24 
25 William H. Orrick
26 United States District Judge
27
28